Криптографија
- девети део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

26. април 2024.

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

Дефиниција

$$E\left(\mathbb{F}_q\right) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \;\middle|\; y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\},$$

где су $a, b \in \mathbb{F}_q$ тд. $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$.

Елиптичке криве над коначним пољима $\mathbb{F}_q$

Надаље: q је степен простог броја $p \neq 2, 3$

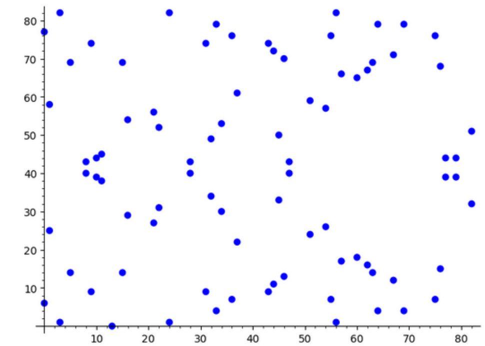
Дефиниција

$$E\left(\mathbb{F}_q\right) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \;\middle|\; y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\},$$

где су $a, b \in \mathbb{F}_q$ тд. $\Delta = -16\left(4a^3 + 27b^2\right) \neq 0$.

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(83), [7,36])
E.plot(pointsize=45)
```



Операције на елиптичкој кривој

- $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$

Операције на елиптичкој кривој

- $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$
- сабирање $P \oplus Q$:
  1. ако је $P = \mathcal{O}$: $\mathcal{O} \oplus Q = Q$
  2. ако је $Q = \mathcal{O}$: $P \oplus \mathcal{O} = P$
  3. ако је $Q = \ominus P \neq \mathcal{O}$: $P \oplus Q = \mathcal{O}$
  4. ако је $P, Q \neq \mathcal{O}$, $Q \neq P, \ominus P$: повучемо праву l кроз P и Q
     - 4.1 или l сече ЕК у још тачно једној тачки R $(\neq P, Q)$
     - 4.2 или је l тангентна на ЕК у једној од тачака P и Q, означимо је са R

     тада је $P \oplus Q = \ominus R$
  5. ако је $P = Q \neq \mathcal{O}, \ominus P$: повучемо тангенту l на ЕК у тачки P, она ће пресећи ЕК у још тачно једној тачки R (различитој од P). Тада је $2P = P \oplus P = \ominus R$

Операције на елиптичкој кривој

- $\ominus P = (x, -y)$ и $\ominus \mathcal{O} = \mathcal{O}$
- сабирање $P \oplus Q$:
  1. ако је $P = \mathcal{O}$: $\mathcal{O} \oplus Q = Q$
  2. ако је $Q = \mathcal{O}$: $P \oplus \mathcal{O} = P$
  3. ако је $Q = \ominus P \neq \mathcal{O}$: $P \oplus Q = \mathcal{O}$
  4. ако је $P, Q \neq \mathcal{O}$, $Q \neq P, \ominus P$: повучемо праву l кроз P и Q
     - 4.1 или l сече ЕК у још тачно једној тачки R $(\neq P, Q)$
     - 4.2 или је l тангентна на ЕК у једној од тачака P и Q, означимо је са R

     тада је $P \oplus Q = \ominus R$
  5. ако је $P = Q \neq \mathcal{O}, \ominus P$: повучемо тангенту l на ЕК у тачки P, она ће пресећи ЕК у још тачно једној тачки R (различитој од P). Тада је $2P = P \oplus P = \ominus R$

Теорема (Групни закон на ЕК)

$(E(\mathbb{F}_q), \oplus, \ominus, \mathcal{O})$ је Абелова група.

Пример: Одредити све тачке Елиптичке криве $y^2 = x^3 + 3x + 8$ на пољем $\mathbb{Z}_{13}$

y	0	± 1	± 2	± 3	± 4	± 5	± 6
y^2	0	1	4	9	3	12	10

Sada možemo da za svako $x \in \{0, 1, 2, \ldots 12\}$ odredimo vrednost za y^2 jednostavnom zamenom vrednosti u jednačinu krive.

$x = 0 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=0.

$x = 1 \to y^2 = 12 \to$ Iz tabele dobijamo da je $y = \pm 5$ pa dobijamo dve tačke krive: (1, 5) i (1, 8).

$x = 2 \to y^2 = 9 \to$ Iz tabele dobijamo da je $y = \pm 3$ pa dobijamo dve tačke krive: (2, 3) i (2, 10).

$x = 3 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=3.

$x = 4 \to y^2 = 6 \to 6$ se ne nalazi u tabeli, stoga nema tačke za x=4.

$x = 5 \to y^2 = 5 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=5.

$x = 6 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=6.

$x = 7 \to y^2 = 8 \to 8$ se ne nalazi u tabeli, stoga nema tačke za x=7.

$x = 8 \to y^2 = 11 \to 11$ se ne nalazi u tabeli, stoga nema tačke za x=8.

$x = 9 \to y^2 = 10 \to$ Iz tabele dobijamo da je $y = \pm 6$ pa dobijamo dve tačke krive: (9, 6) i (9, 7).

$x = 10 \to y^2 = 11 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=10.

$x = 11 \to y^2 = 7 \to 5$ se ne nalazi u tabeli, stoga nema tačke za x=11.

$x = 12 \to y^2 = 4 \to$ Iz tabele dobijamo da je $y = \pm 2$ pa dobijamo dve tačke krive: (12, 2) i (12, 11).

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$$

Израчунати $\underbrace{(1,8)}_{P} \oplus \underbrace{(9,7)}_{Q}$ на ел. кривој $E: y^2 = x^3 + 3x + 8$ над $\mathbb{Z}_{13}$

Сав рачун mod 13:

Права l која садржи P и Q: $y - 8 = \frac{8-7}{\underbrace{1-9}}(x-1)$ $\quad$ тј. $y - 8 = 8(x-1)$

$$= \frac{1}{-8} = \frac{1}{5} = 8 \qquad\qquad y = 8x$$

$E \cap l$: $(8x)^2 = x^3 + 3x + 8$

$$x^3 \underbrace{-64}_{+1} x^2 + 3x + 8 = 0 \qquad\qquad P \oplus Q = \ominus R$$

Вијетова правила $\underset{\overset{\parallel}{1}}{x_P} + \underset{\overset{\parallel}{9}}{x_Q} + x_R = -1$

$$x_R = -11 = 2$$

$$y_R = 8 \cdot 2 = 3$$

$$P \oplus Q = (2, -3) = (2, 10)$$

Израчунати $2(9,7)$ на ел. кривој $E: y^2 = x^3 + 3x + 8$ над $\mathbb{Z}_{13}$

Сав рачун mod 13:

Тангента на E у тачки P: $y - 7 = f'(9)(x-9)$ тј: $y - 7 = 12(x-9)$

$$= 12x + 9$$

$$y = 12x + 16$$

$$= -x + 3$$

$y = f(x) = \sqrt{x^3 + 3x + 8}$

(део E који $\ni P$)

$$f'(x) = \frac{3x^2+3}{2\sqrt{x^3+3x+8}} = \frac{3x^2+3}{2y}$$

$$\underset{\uparrow_P}{f'(9)} = \frac{3\cdot 81 + 3}{2\cdot 7} = \frac{3\cdot 3+3}{1} = 12$$

$E \cap l$: $(-x+3)^2 = x^3 + 3x + 8$

$$x^3 - x^2 + \dots = 0$$

$2P = \ominus R$

Вијетова правила $\Rightarrow$ $\underset{2\cdot 9 = 5}{2x_P} + x_R = +1$

$$x_R = 1 - 5 = 9$$

$$y_R = -9 + 3 = -6$$

$$2P = (9, 6)$$

Таблица сабирања на кривој $y^2 = x^3 + x + 2$ на пољем $\mathbb{Z}_{13}$

+	∞	(1.2)	(1.11)	(2.5)	(2.8)	(6.4)	(6.9)	(7.1)	(7.12)	(9.5)	(9.8)	(12.0)
∞	∞	(1.2)	(1.11)	(2.5)	(2.8)	(6.4)	(6.9)	(7.1)	(7.12)	(9.5)	(9.8)	(12.0)
(1.2)	(1.2)	(12.0)	∞	(6.9)	(7.1)	(2.8)	(9.5)	(9.8)	(2.5)	(7.12)	(6.4)	(1.11)
(1.11)	(1.11)	∞	(12.0)	(7.12)	(6.4)	(9.8)	(2.5)	(2.8)	(9.5)	(6.9)	(7.1)	(1.2)
(2.5)	(2.5)	(6.9)	(7.12)	(9.8)	∞	(1.11)	(6.4)	(1.2)	(7.1)	(2.8)	(12.0)	(9.5)
(2.8)	(2.8)	(7.1)	(6.4)	∞	(9.5)	(6.9)	(1.2)	(7.12)	(1.11)	(12.0)	(2.5)	(9.8)
(6.4)	(6.4)	(2.8)	(9.8)	(1.11)	(6.9)	(2.5)	∞	(9.5)	(12.0)	(1.2)	(7.12)	(7.1)
(6.9)	(6.9)	(9.5)	(2.5)	(6.4)	(1.2)	∞	(2.8)	(12.0)	(9.8)	(7.1)	(1.11)	(7.12)
(7.1)	(7.1)	(9.8)	(2.8)	(1.2)	(7.12)	(9.5)	(12.0)	(2.5)	∞	(1.11)	(6.9)	(6.4)
(7.12)	(7.12)	(2.5)	(9.5)	(7.1)	(1.11)	(12.0)	(9.8)	∞	(2.8)	(6.4)	(1.2)	(6.9)
(9.5)	(9.5)	(7.12)	(6.9)	(2.8)	(12.0)	(1.2)	(7.1)	(1.11)	(6.4)	(9.8)	∞	(2.5)
(9.8)	(9.8)	(6.4)	(7.1)	(12.0)	(2.5)	(7.12)	(1.11)	(6.9)	(1.2)	∞	(9.5)	(2.8)
(12.0)	(12.0)	(1.11)	(1.2)	(9.5)	(9.8)	(7.1)	(7.12)	(6.4)	(6.9)	(2.5)	(2.8)	∞

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост

Теорема

Нека је p непаран прост

1. Ако $p \nmid a$ број решења квадратне конгруенције $x^2 \equiv_p a$ је 0 или 2 (каже се: a је квадратни неостатак или остатак, редом)
2. Број квадратних (не)остатака је $\frac{p-1}{2}$

Колико има тачака на кривој $E(\mathbb{F}_q)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост

Теорема

Нека је p непаран прост

1. Ако $p \nmid a$ број решења квадратне конгруенције $x^2 \equiv_p a$ је 0 или 2 (каже се: a је квадратни неостатак или остатак, редом)
2. Број квадратних (не)остатака је $\frac{p-1}{2}$

Доказ:

1. Ако је x_0 решење, онда је $p - x_0$ друго решење.
   И ово су сва решења јер из $x_1^2 \equiv_p a \equiv_p x_2^2$ следи $p \,\middle|\, x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$, па p дели једну од заграда
2. Ако $x^2 \equiv_p a$ гледамо као једначину по две променљиве x и a из $\mathbb{Z}_p^\times$ она има $p - 1$ решење $= 2 \cdot$ бр. кв. ост. $+\ 0 \cdot$ бр. кв. неост.

Колико има тачака на кривој $E\left(\mathbb{F}_q\right)$, тј. $(x, y) \in \mathbb{F}_q$ тд. $y^2 = x^3 + ax + b$?

- да поједноставимо $q = p$ прост

Теорема

Нека је p непаран прост

1. Ако $p \nmid a$ број решења квадратне конгруенције $x^2 \equiv_p a$ је 0 или 2 (каже се: a је квадратни неостатак или остатак, редом)
2. Број квадратних (не)остатака је $\frac{p-1}{2}$

Доказ:

1. Ако је x_0 решење, онда је $p - x_0$ друго решење.
   И ово су сва решења јер из $x_1^2 \equiv_p a \equiv_p x_2^2$ следи $p \left| x_1^2 - x_2^2 = \left(x_1 - x_2\right)\left(x_1 + x_2\right)\right.$, па p дели једну од заграда
2. Ако $x^2 \equiv_p a$ гледамо као једначину по две променљиве x и a из $\mathbb{Z}_p^\times$ она има $p - 1$ решење $= 2 \cdot$ бр. кв. ост. $+ \, 0 \cdot$ бр. кв. неост.

- Ускоро: брза провера да ли је a квадратни (не)остатак

Колико има тачака на кривој $E(\mathbb{F}_p)$, тј. $(x, y) \in \mathbb{F}_p$ тд. $y^2 = x^3 + ax + b$?

Колико има тачака на кривој $E(\mathbb{F}_p)$, тј. $(x, y) \in \mathbb{F}_p$ тд. $y^2 = x^3 + ax + b$?

- Интуитивно:

$$\underbrace{1}_{\mathcal{O}} + \begin{array}{c}\text{број реш.}\\ \text{по } x,\ y\end{array} = 1 + \sum_{x \in \mathbb{F}_p} \begin{array}{c}\text{број реш. по}\\ y \text{ за фикс. } x\end{array} = \star$$

Колико има тачака на кривој $E(\mathbb{F}_p)$, тј. $(x, y) \in \mathbb{F}_p$ тд. $y^2 = x^3 + ax + b$?

- Интуитивно:

$$\underbrace{1}_{\mathcal{O}} + \begin{array}{c}\text{број реш.}\\ \text{по } x,\ y\end{array} = 1 + \sum_{x \in \mathbb{F}_p} \begin{array}{c}\text{број реш. по}\\ y \text{ за фикс. } x\end{array} = \star$$

- Суманд узима насумично (подједнако вероватно) вредности 0 или 2, статистички: очекивање је 1

$$\star \approx 1 + \sum_{x \in \mathbb{F}_p} 1 = p + 1$$

Хасеова теорема

Кардиналност групе $E\left(\mathbb{F}_q\right)$ je $q+1+s$, где je $s \leqslant 2\sqrt{q}$.
Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E\left(\mathbb{F}_q\right)$ тд. je $\left|E\left(\mathbb{F}_q\right)\right| = q+1+s$

Хасеова теорема

Кардиналност групе $E\left(\mathbb{F}_q\right)$ је $q+1+s$, где је $s \leqslant 2\sqrt{q}$.
Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E\left(\mathbb{F}_q\right)$ тд. је $\left|E\left(\mathbb{F}_q\right)\right| = q+1+s$

Кључна идеја:

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$

Хасеова теорема

Кардиналност групе $E\left(\mathbb{F}_q\right)$ је $q+1+s$, где је $s \leqslant 2\sqrt{q}$. Додатно, за сваку целобројну вредност $s \in [-2\sqrt{q}, 2\sqrt{q}]$ постоји ЕК $E\left(\mathbb{F}_q\right)$ тд. је $\left|E\left(\mathbb{F}_q\right)\right| = q+1+s$

Кључна идеја:

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Уместо фиксне кардиналности $q-1$ имамо слободу $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$

Помоћу Sage-а можемо наћи тачке са елиптичких кривих над $\mathbb{Z}_7$ (видимо да њихов број није увек исти!)

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[1,3])
E.points()
```

```
[(0 : 1 : 0), (4 : 1 : 1), (4 : 6 : 1), (5 : 0 : 1), (6 : 1 : 1), (6 : 6 : 1)]
```

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[2,6])
E.points()
```

```
[(0 : 1 : 0), (1 : 3 : 1), (1 : 4 : 1), (2 : 2 : 1), (2 : 5 : 1), (3 : 2 : 1), (3 : 5 : 1), (4 : 1
: 1), (4 : 6 : 1), (5 : 1 : 1), (5 : 6 : 1)]
```

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[6,6])
E.points()
```

```
[(0 : 1 : 0), (3 : 3 : 1), (3 : 4 : 1), (5 : 0 : 1)]
```

- Уместо групе $(\mathbb{F}_q^*, \cdot)$ користити групу $(E(\mathbb{F}_q), \oplus)$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- Уместо групе $\left(\mathbb{F}_q^*, \cdot\right)$ користити групу $\left(E\left(\mathbb{F}_q\right), \oplus\right)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

- Уместо групе $(\mathbb{F}_q^*, \cdot)$ користити групу $(E(\mathbb{F}_q), \oplus)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

Проблем дискретног логаритма

Ако је познато P и nP одредити n.

- Уместо групе $(\mathbb{F}_q^*, \cdot)$ користити групу $(E(\mathbb{F}_q), \oplus)$
- Степеновање g^n се мења са $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$
- Приметимо да nP може бити и $\mathcal{O}$
- nP се рачуна поновљеним дуплирањем тачке (као поновљено квадрирање)
  - Пример: За $100P$ запишемо бинарно $100 = 2^6 + 2^5 + 2^2 = \overline{1100100}_2$, тада је

$$100P = 2(2(P \oplus 2(2(2(P \oplus 2P)))))$$

- nP се рачуна са $O(\log n)$ операција $\oplus$, а сваки $\oplus$ се реализује са неколико сабирања, одузимања, множења...

Проблем дискретног логаритма

Ако је познато P и nP одредити n.

У пракси, ово се решава још спорије од дискретног логаритма у $\mathbb{F}_q^*$

За елиптичку криву $y^2 = x^3 + 2x + 6$ над $\mathbb{Z}_7$ добијамо цикличну групу реда 11 чији је генератор $P = (1, 4)$

Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[2,6])
E.points()
```

```
[(0 : 1 : 0), (1 : 3 : 1), (1 : 4 : 1), (2 : 2 : 1), (2 : 5 : 1), (3 : 2 : 1), (3 : 5 : 1), (4 : 1
: 1), (4 : 6 : 1), (5 : 1 : 1), (5 : 6 : 1)]
```

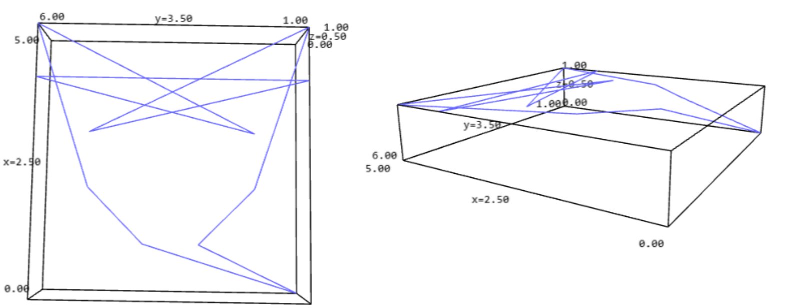
Save Copy Run SageMath 10.1

```
E = EllipticCurve(GF(7),[2,6])
P=E([1,4])
s=[n*P for n in range(1,12)]
s
```

```
[(1 : 4 : 1),
 (2 : 5 : 1),
 (5 : 6 : 1),
 (3 : 2 : 1),
 (4 : 6 : 1),
 (4 : 1 : 1),
 (3 : 5 : 1),
 (5 : 1 : 1),
 (2 : 2 : 1),
 (1 : 3 : 1),
 (0 : 1 : 0)]
```

Save Copy Run Sage-10.1

```
E=EllipticCurve(GF(7),[2,6])
P=E([1,4])
s=[n*P for n in range(1,13)]
plot(line(s))
```



Изломљена линија спаја P, $2P$, $\ldots$, $10P$, $11P = \mathcal{O}$ и $12P = P$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m који се преводе у нумерички еквивалент M (као раније). Максимална величина блока N је таква да $Nk < q$

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m који се преводе у нумерички еквивалент M (као раније). Максимална величина блока N је таква да $Nk < q$
- M треба кодирати тачком (x_0, y_0) са криве $E:\ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m који се преводе у нумерички еквивалент M (као раније). Максимална величина блока N је таква да $Nk < q$
- M треба кодирати тачком (x_0, y_0) са криве $E: \; y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m који се преводе у нумерички еквивалент M (као раније). Максимална величина блока N је таква да $Nk < q$
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- Уколико претх. нема решења покушавамо даље са $Mk + 1$, $Mk + 2$, $\ldots$, $Mk + k - 1$ све док не пронађемо (x_0, y_0)

Кодирање података помоћу ЕК

Ако је $q = p$ прост број:

- Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- Порука која треба да се кодира се по потреби се дели на блокове m који се преводе у нумерички еквивалент M (као раније). Максимална величина блока N је таква да $Nk < q$
- M треба кодирати тачком (x_0, y_0) са криве $E: \ y^2 = x^3 + ax + b$ (над $\mathbb{Z}_p$)
- Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- Уколико претх. нема решења покушавамо даље са $Mk + 1$, $Mk + 2, \ldots, Mk + k - 1$ све док не пронађемо (x_0, y_0)
- Квадратна конгруенција има решење у $\frac{1}{2}$ случајева, па је вероватноћа да ћемо у k покушаја бар једном бити успешни $1 - \frac{1}{2^k}$

Општи случај: $q = p^\alpha$ и

$\mathbb{F}_q \cong \left\{ a_0 + a_1 t + \cdots + a_{\alpha-1} t^{\alpha-1} \;\middle|\; 0 \leqslant a_0, a_1, \ldots, a_{\alpha-1} \leqslant p-1 \right\}$

- Све исто као на прошлом слајду сем:
  - Када се кодира M број $Mk + j$ (редом за $j = 0, 1, \ldots, k-1$) се запише у основи p као

    $$Mk + j = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

    ($r \leqslant \alpha - 1$ јер је $M < q$) и покуша се да се за полином $x_0 = x_0(t) = a_0 + a_1 t + \cdots + a_{r-1} t^{r-1}$ нађе полином $y_0 = y_0(t)$ тд. (x_0, y_0) припада ЕК

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$
  - Објашњење: $\left[\frac{x_0}{k}\right] = \left[M + \frac{j}{k}\right] = M$ (не знамо шта је j, само знамо да је из $[0, k-1]$)

Декодирање података помоћу ЕК

Имамо тачку (x_0, y_0), треба реконструисати поруку m:

- За $q = p$ прост: M добијамо као $\left[\frac{x_0}{k}\right]$
  - Објашњење: $\left[\frac{x_0}{k}\right] = \left[M + \frac{j}{k}\right] = M$ (не знамо шта је j, само знамо да је из $[0, k-1]$)
- За $q = p^\alpha$: имамо додатно корак да полином $x_0(t) = a_0 + a_1 t + \cdots + a_{r-1} t^{r-1}$ преведемо у број $a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}$, даље аналогно претх. случају

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \; y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \ y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \; y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- Затим рачунају јавне кључеве $a_A P, a_B P \in E(\mathbb{F}_q)$ и размењују их (објављују)

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \ y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- Затим рачунају јавне кључеве $a_A P, a_B P \in E(\mathbb{F}_q)$ и размењују их (објављују)
- Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E:\ y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- Затим рачунају јавне кључеве $a_A P, a_B P \in E(\mathbb{F}_q)$ и размењују их (објављују)
- Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$
- Алиса може да израчуна K као $K = a_A(a_B P)$. И слично Бобан долази до K

Дифи-Хелманово усаглашавање кључа помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \ y^2 = x^3 + ax + b$ над $\mathbb{F}_q$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- Затим рачунају јавне кључеве $a_A P, a_B P \in E(\mathbb{F}_q)$ и размењују их (објављују)
- Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$
- Алиса може да израчуна K као $K = a_A(a_B P)$. И слично Бобан долази до K
- Цица види само $a_A P$ и $a_B P$, не и K

Zadatak *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je* $E: y^2 = x^3 + 3x + 8$ *nad poljem* $\mathbb{F}_{13}$. *Ako se koristi generator* $P = (2, 3)$, *tajni ključevi* $a_A = 4$, $a_B = 5$, *odrediti tačku koja se dobija kao rezultat usaglašavanja.*

Save Copy Run SageMath 10.1

```
E=EllipticCurve(GF(13), [3,8])
P=E([2,3])
a_A=4
a_B=5
a_AP=a_A*P
a_BP=a_B*P
AlisinK=a_A*a_BP
BobanovK=a_B*a_AP
P, a_AP, a_BP, AlisinK, BobanovK
```

```
((2 : 3 : 1), (1 : 5 : 1), (1 : 8 : 1), (12 : 11 : 1), (12 : 11 : 1))
```

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E:\ y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \; y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E: \ y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E:\ y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- Бобан тачку keP може добити тако што kP помножи са e

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E:\ y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- Бобан тачку keP може добити тако што kP помножи са e
- Бобан сабира тачке $M \oplus keP$ и $\ominus keP$ и долази до M

ЕлГамалов криптосистем помоћу ЕК

- Јавни кључ: коначно поље $\mathbb{F}_q$, елиптичка крива $E:\ y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
  - Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- Бобан тачку keP може добити тако што kP помножи са e
- Бобан сабира тачке $M \oplus keP$ и $\ominus keP$ и долази до M
- Цица види само eP и kP, $M \oplus keP$ и мора да реши пробем дискретног логаритма да би дошла до поруке M

Zadatak *Za sistem El Gamal koristi se eliptička kriva* $E : y^2 = x^3 + 3x + 8$ *nad poljem* $\mathbb{F}_{13}$. *Generator je* $P = (2,3)$. *Ako su tajni ključ* $e = 5$, *prikazati postupak šifrovanja poruke* $M = (12,11)$ *(koristi se slučajan broj* $k = 4$*), a zatim postupak dešifrovanja šifrata.*

Save Copy Run SageMath 10.1

```
E=EllipticCurve(GF(13),[3,8])
P=E([2,3])
e=5
M=E([12,11])
k=4
eP=e*P
kP=k*P
kriptM=M+k*eP
dekriptM=kriptM-e*kP
eP, kP, kriptM, dekriptM
```

```
((1 : 8 : 1), (1 : 5 : 1), (1 : 5 : 1), (12 : 11 : 1))
```

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E\left(\mathbb{Z}_n\right)$ и неку тачку P са те криве

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

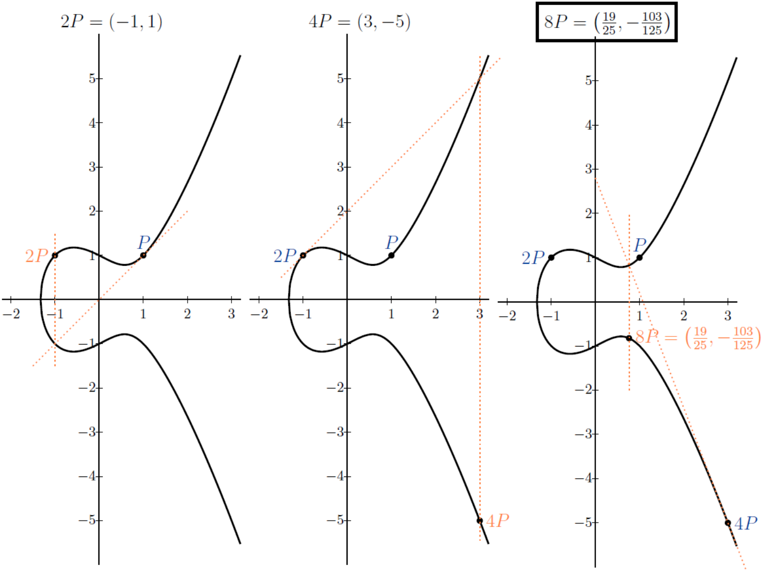
- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E\left(\mathbb{Z}_n\right)$ и неку тачку P са те криве
- Кренемо да рачунамо $2P$, $3P$, $4P$, $\ldots$ (или $2P$, $4P$, $8P$, $\ldots$) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
  - Практично рачунамо све у $\mathbb{Q}$, па редукујемо $\bmod n$

Факторизација помоћу ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- Претпоставимо супротно: n је прост
- Онда је $\mathbb{Z}_n$ поље
- Изаберемо неку елиптичку криву $E\left(\mathbb{Z}_n\right)$ и неку тачку P са те криве
- Кренемо да рачунамо $2P$, $3P$, $4P$, $\ldots$ (или $2P$, $4P$, $8P$, $\ldots$) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
  - Практично рачунамо све у $\mathbb{Q}$, па редукујемо $\bmod n$
- Када се у имениоцу појави број g који није инвертибилан по модулу n, онда ће НЗД$(g, n) > 1$ бити прави делилац n

Пример: За растављање 35 користимо ЕК $y^2 = x^3 - x + 1$ над $\mathbb{Z}_{35}$ (није поље) и $P = (1,1)$



НЗД$(35, 25) = 5$ је делилац 35

Example

We want to factor 4453. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \bmod 4453$ and let $P = (1, 3)$. Let's try to compute $3P$. First, we compute $2P$. The slope of the tangent line at P is

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

We used the fact that $\gcd(6, 4453) = 1$ to find $6^{-1} \equiv 3711 \pmod{4453}$. Using this slope, we find that $2P = (x, y)$, with

$$x \equiv 3713^2 - 2 \equiv 4332, \quad y \equiv -3713(x - 1) - 3 \equiv 3230.$$

To compute $3P$, we add P and $2P$. The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But $\gcd(4331, 4453) = 61 \neq 1$. Therefore, we cannot find $4331^{-1} \pmod{4453}$, and we cannot evaluate the slope. However, we have found the factor 61 of 4453, and therefore $4453 = 61 \cdot 73$.

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m = \text{НЗС}(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m =$ НЗС$(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- знамо да $|E(\mathbb{Z}_p)|$ дели ове m, па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p

Ленстрин метод

- У примерима смо имали среће да међу mP-овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B-гладак број за неко мало B (инспирисано Полардовим $(p-1)$-методом)
- не погађати које m ради, већ покушати са $m =$ НЗС$(1, 2, \ldots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- знамо да $|E(\mathbb{Z}_p)|$ дели ове m, па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p
- али нећемо рачунати $\bmod p$, већ $\bmod n$

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом
- ако се као именилац појави g дељив са n - променити тачку P

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ако успемо да израчунамо mP без проблема - претпоставка о B-глаткости није испуњена, покушати са већим B или другом елиптичом кривом
- ако се као именилац појави g дељив са n - променити тачку P
- ако се као именилац појави g које није дељиво са n, али није ни инвертибилно по модулу n - онда је НЗД(g, n) прави делилац n